REMARKS

Claims 1-7 and 9-21 are pending in this application. By this amendment, claims 1 and 7 are amended. Reconsideration and allowance in view of the following remarks are respectfully requested.

In the present Amendment, the claims have been amended to further clarify the claimed invention. Applicant submits that in general Applicant does not believe the various amendments to be narrowing to the amended claims. Rather, Applicant submits that the amendments simply draw out what was already found, either explicitly or implicitly, in the claims.

I. THE CLAIMS DEFINE PATENTABLE SUBJECT MATTER

A. The Rejection of Claims 1-4, 6, 7, 9-15, 17 and 19-21

In paragraph 4, the pending Office Action rejects claims 1-4, 6, 7, 9-15, 17 and 19-21 under 35 U.S.C. 102(e) as being anticipated by Freund, U.S. Patent No. 5,987,611 (Freund). This rejection is respectfully traversed.

Claim 1 recites a method for providing accessibility to a plurality of remote service providers across a network via a single login to a host service provider, each of the plurality of remote service providers being accessible through the host service provider and each of the plurality of remote service providers having separate login procedures requiring data, the method comprising the steps of the host service provider receiving the single login from a user, the host service provider having a universal session manager; the universal session manager retrieving data from a validation database based on the single login to the host service provider, wherein the data is effective for accessing a selected one of the plurality of remote service providers, and wherein the data is based at least in part on the single login; the universal session manager transmitting said data to the remote service provider, the universal session manager and the

remote service provider exchanging the data to effect a two-sided authentication; and the host service provider directing the user to the remote service provider.

The Examiner is respectfully requested to reconsider and withdraw the rejection as set out in the Office Action. As reflected in claim 1, the teachings of Freund are substantially different then the present invention.

In paragraph 4, the Office Action alleges various assertions as to the manner in which Freund allegedly teaches the claimed invention. The Office Action asserts that as to claim 1, Freund discloses a method for accessing one of a plurality of remote service providers (web server 350's of fig. 3B can be Internet Service providers) across a network via a single login to a host service provider (320a fig. 3B), each of the plurality of remote service providers being accessible through the host service provider, and each of the plurality service providers having separate login procedures requiring data comprising (as set forth in the Office Action) the steps of:

- The host service provider (320a fig. 313) receiving the single login (providing remote login from clients 310's fig. 3A), the host service provider (see abstract, fig. 3B, col. 21 line 47 to col. 22 line 21);
- transmitting data to the remote service provider and directing the user to the remote service provider after the remote service provider exchanging the data to effect a two-sided authentication and the host service provider directing the user to the remote service provider (using authentication server 371 fig. 313 for checking client/user ID and password, see col. 22 lines 1-59); and
- a universal session manager (373 fig. 3B) retrieving data from a validation database (374 fig. 3B) based on the single login, wherein the data is effective for accessing a

remote service provider and is based at least in part on the received username and password (i.e., monitoring user access, col. 22 line 23 to col. 23 line 55).

These assertions as set forth in the Office Action are respectfully traversed. For the reasons set forth herein, Freund fails to teach the invention as recited in claim 1. Freund is directed to a system and methodology for managing internet access on a per application basis for client computers connected to the internet. Applicant respectfully submits that this title is representative, and that Freund relates to Internet access - and is different than the claimed invention.

The features of claim 1 are noted above. Applicant submits that Freund, in particular, fails to teach the claimed interrelationship between the universal session manager, the host service provider and the remote service provider, as recited in claim 1.

As to the more general teachings of Freund's invention, in column 8, lines 40-65, Freund describes an Internet access monitoring system including that: (1) The system should preferably be capable of restricting access to the Internet (or other Wide Area Network) to certain approved applications or/and application versions. (2) The system should preferably support centrally-maintained access rules (e.g., defining basic access rights), but at the same time allow individual workgroup managers or even individual users to set rules for their area of responsibility, if so desired by the organization. (3) The system should preferably prevent users from circumventing Internet access rules, either accidentally or intentionally. Freund describes that it should be difficult, for instance, for a user to circumvent access rules by connecting to the Internet through a dial-up connection (e.g., connecting to an ISP with a modem). Similarly, it should be difficult for a user to circumvent access rules by uninstalling or tampering with components of the system, from his/her own PC.

Freund teaches further aspects relating to Internet access in column 10, lines 55-65. Freund teaches that the ability to monitor and regulate Internet access on a per application basis is particularly advantageous. Advantages include, for instance, the ability to specify which applications can (and cannot) access the Internet. Freund describes that IS departments have a strong interest in limiting the number of applications used on their LANs, including limiting available applications to a uniform set of "approved" applications. For one, user support is simplified if fewer different applications are in use. Further, Freund teaches, the overall integrity of one's corporate networks is improved if known applications (or unknown versions of applications) are used.

In the 35 U.S.C. §102 rejection set forth in the Office Action, the Office Action refers to the teachings of Freund in columns 21 and 22. In column 22, lines 7-21, for example, Freund teaches that in an embodiment of Freund, the ISP installs an additional central server component 370 to host the central supervisor application; this new component comprises an ISP authentication server 371 and an ISP supervisor server 372 (which includes a central supervisor application 373). After the central ISP authentication server 371 has established the authenticity of the user, it contacts the central supervisor application 373 in order to find out if the user has established additional access monitoring services. In such a case, the ISP authentication server 371 signals the POP server 320a to only allow limited access to the Internet and redirect all requests to a "Sandbox" server application, shown at 374, on the central supervisor server 372. This "Sandbox" server 374 restricts the client's Internet access to a very limited account maintenance site. Aspects of the sandbox server 374 vis-à-vis the rejection are discussed further below.

In conjunction with the other features, claim 1 of the present invention recites the host service provider having a universal session manager, the universal session manager retrieving data from a validation database based on the single login to the host service provider, wherein the data is effective for accessing a selected one of the plurality of remote service providers, and wherein the data is based at least in part on the single login. Of particular note vis-à-vis the teachings of Freund, claim 1 recites the universal session manager transmitting said data to the remote service provider, the universal session manager and the remote service provider exchanging the data to effect a two-sided authentication; and the host service provider directing the user to the remote service provider.

Thus, claim 1 recites a particular interrelationship between the universal session manager and the remote service provider. Freund fails to teach this interrelationship.

The Office Action alleges that "Freund discloses a method for accessing one of a plurality of remote service providers (web server 350's of fg.3B can be Internet Service providers)". Accordingly, the Office Action is interpreting the web servers 350 of Fig. 3B to be the claimed remote service provider. This interpretation is also followed in the rejection of independent claim 7.

Further, the Office Action asserts that Freund teaches transmitting data to the remote service provider and directing the user to the remote service provider after the remote service provider exchanging the data to effect a two-sided authentication and the host service provider directing the user to the remote service provider (using authentication server 371 fig.313 for checking client/user ID and password). The Office Action refers to col. 22 lines 1-59 of Freund.

Applicant submits that this portion of the rejection in particular reflects the deficiencies of Freund vis-à-vis the claimed invention. That is, claim 1 recites "the universal session

manager and the remote service provider exchanging the data to effect a two-sided authentication." The Office Action asserts that the web servers 350 are the remote service providers. Also, of note, the Office Action asserts that the supervisor 373 of Freund is the claimed universal session manager. Applicant submits that Freund fails to teach or suggest the supervisor 373 and the web servers 350 exchanging data to effect a two-sided authentication, as recited in claim 1. The Office Action appears to assert that such teaching is in column 22 of Freund. However, such portion of Freund appears devoid of any such teaching.

In column 22, lines 21-34, Freund does teach that the Client Monitor on the client PC (e.g., monitor 311a) monitors the log-on process. Once the limited access to the Internet is established, the monitor contacts the central supervisor application 373 on the ISP supervisor server 372 in order to receive access rules and other required components. Freund describes that once the central supervisor application 373 is satisfied that the Client Monitor has received the appropriate access rules and is working satisfactory, it contacts the POP server 320a to signal that the user now has full Internet access. The central supervisor application 373 will continue to check the Client Monitor and, in case of any problems, signals the POP server 320a to fall back to limited access to the Internet. However, such teaching of Freund fails to disclose any interrelationship of the supervisor 373 vis-à-vis the web server 350, so as to teach or suggest the claimed invention.

Freund does teach aspects of the web servers 350 in column 15, lines 1-11, for example. Freund teaches that a firewall 330 may be implemented in a conventional manner, such as employing a router-based or server-based firewall process for monitoring communications with various Web servers 350 connected to the Internet 340. However, Freund fails to teach the interrelationship between the various components as recited in claim 1 and discussed above.

As a further note, the Office Action asserts in the rejection that a universal session manager (373 fig.3B) retrieving data from a validation database (374 fig.3B) based on the single login, wherein the data is effective for accessing a remote service provider. Applicant respectfully requests that the Examiner more clearly set forth the support for such assertion. That is, Freund teaches in column 22 that the ISP authentication server 371 signals the POP server 320a to only allow limited access to the Internet and redirect all requests to a "Sandbox" server application, shown at 374, on the central supervisor server 372. Freund teaches that this "Sandbox" server 374 restricts the client's Internet access to a very limited account maintenance site. Freund further teaches in column 22, lines 35-41, that if the user does not have a Client Monitor installed, or the Client Monitor is not functioning or has been tampered with, the user will only have access to the "Sandbox" server 374. The user will not gain access to the rest of the Internet until the user downloads the Client Monitor component from the "Sandbox" server 374 or otherwise reinstall the Client Monitor application. However, such disclosure of Freund is not seen to teach "a universal session manager (373 fig.3B) retrieving data from a validation database (374 fig.3B) based on the single login, wherein the data is effective for accessing a remote service provider" - as alleged in support of the rejection. The Examiner is requested to either clarify or withdraw such assertion.

Applicant respectfully submits that Freund fails to teach or suggest the features of claim 1 for at least the reasons set forth above. Further, claim 7 is allowable at least for some of the reasons discussed above with respect to claim 1. Further, the various dependent claims recite patentable subject matter at least for their various dependencies on claims 1 and 7, as well as for the additional subject matter recited in such dependent claims.

B. The Rejection of Claims 5, 16 and 18 under 35 U.S.C. §103

In the Office Action, claims 5, 16 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freund as in item 4 above and in view of Kirsch U.S. Patent No. 5,963,915.

The Office Action asserts that Freund does not specifically disclose a triple handshake and a cookie, but that however, Kirsch discloses a triple handshake and a cookie (i.e., providing a cookie and a series of handshake transactions to negotiate the establishment of the secure transactions between the servers, see col. 2 lines 1-46 and col. 8 lines 12-63). The Office Action further alleges that it would have been obvious to one of the ordinary skill in the art at the time the invention was made to implement Kirsch's teachings into the computer system of Freund to process data transaction over the Internet because it would have provided automatic simultaneous purchase transactions handling for both secure and insecure client browsers and increased levels of authentication of data communications in the Internet.

Illustratively, Kirsch teaches in column 4, lines 48-64, that the Kirsch invention provides for a purchase transaction that appears to the client user as a singular selection of a purchasable product or service and a singular confirmation of the purchase. A persistent predetermined coded identifier is established on the client browser corresponding to an account record stored by the merchant server. Kirsch further teaches that a predetermined URL referencing a purchasable product or service is served to the client browser.

Further, Kirsch teaches that a facility known as persistent client-side cookies has been introduced to provide a way for server systems to store selected information on client systems. Cookies are created at the discretion of the server system in response to specific client URL requests. Part of the server response is a cookie consisting of a particularly formatted string of text including a cookie identifier, a cookie path, a server domain name and, optionally, an expiration date, and a secure marker. Kirsch further describes that a conventional uniform

resource locator (URL), utilizing "https" as the secure HTTP protocol identifier, is issued by the client browser to specifically request a secure client/server session. A series of handshake transactions are provided to negotiate the establishment of the secure session including performing an encryption key exchange that is used in an encryption algorithm implemented by both the client-side and server-side secure sockets layers.

However, Applicant submits that even if it were obvious to somehow use Kirsch's teachings relating to cookies and authorization techniques, which Applicant does not admit to be the case, to modify Freund, such combination would still fail to teach or suggest the claimed invention.

It is submitted that Freund and Kirsch, either alone or in combination, fail to teach or suggest the claimed invention. Withdrawal of the 35 U.S.C. §103 rejection is respectfully requested.

II. CONCLUSION

For at least the reasons outlined above, Applicant respectfully asserts that the application is in condition for allowance. Favorable reconsideration and allowance of the claims are respectfully solicited.

For any fees due in connection with filing this Response the Commissioner is hereby authorized to charge the undersigned's Deposit Account No. 50-0206.

Application Serial No.: 09/591,687 Attorney Docket No.: 47004.000074

Should the Examiner believe anything further is desirable in order to place the application in even better condition for allowance, the Examiner is invited to contact Applicant's undersigned representative at the telephone number listed below.

Respectfully submitted,
HUNTON & WILLIAMS

James R. Miner
Registration No. 40,444

Hunton & Williams
1900 K Street, N.W., Suite 1200
Washington, D.C. 20006-1109
(202) 955-1500

Dated: **March 30, 2005**